MASTER OF SCIENCE
IN
SYSTEMS ENGINEERING

ANALYSIS OF JAMMER RESISTANT, SPREAD SPECTRUM, VSAT COMMUNICATION SCHEME FOR MARITIME PLATFORM USING DS-CDMA

Ersin Aras-Lieutenant Junior Grade, Turkish Navy
B.S., Turkish Naval Academy, 1996
Master of Science in Systems Engineering-September 2002
Advisor: Tri T. Ha, Department of Electrical and Computer Engineering
Second Reader: Herschel H. Loomis, Jr., Department of Electrical and Computer Engineering

In this thesis, a new VSAT (Very Small Aperture Terminal) communication system is developed using Direct Sequence Code Division Multiple Access (DS-CDMA) for multiple maritime mobile users in the footprint of national communication satellites. The Forward Error Correction (FEC) is implemented by applying convolution encoding with soft decision decoding. The worst-case scenario is always considered by placing VSAT system and different types of jammers on the footprint where the minimum signal-to-noise ratio is possible. Using this assumption, the performance of the system is analyzed for different convolution code rates, for a different number of users and for the different jammer powers. The Walsh codes are used to establish an orthogonal cover between CDMA channels in a VSAT. Additionally, spread spectrum is included by PN sequences to ensure as much orthogonal coverage as possible between the VSATs. Also, that spreading is the key to minimizing these hostile jammer effects. After analyzing VSAT system for possible scenario elements, optimum system parameters are introduced for military and civilian applications.

KEYWORDS: VSAT, Satellite Communications, CDMA, Spread Spectrum, Performance Analysis, Link Budget, Link Margin, Pulse Jamming, Tone Jamming, Walsh Functions, PN Sequences, Convolutional Codes, Forward Error Correction, Channel Distances, Gaussian Approximation

MIXED SIGNAL PROCESSOR FOR A ROBUST SYMMETRICAL NUMBER SYSTEM DIRECTION FINDING ANTENNA

Charles F. Babb-Lieutenant, United States Navy
B.S., Auburn University, 1995
Master of Science in Systems Engineering-September 2002
Advisor: Phillip E. Pace, Department of Electrical and Computer Engineering
Co-Advisor: David C. Jenn, Department of Electrical and Computer Engineering

This applied research project has designed, simulated, constructed and tested the performance of a processing system for a prototype direction finding antenna. A mixed signal architecture to derive the direction of arrival from a Robust Symmetrical Number System (RSNS) encoded direction finding array is based on a new phase sampling interferometer approach that can be easily incorporated into established techniques to provide a high resolution, small-baseline array with few number of phase sampling comparators. The approach is based on preprocessing the received signal using the RSNS. The preprocessing is used to decompose the spatial filtering operation into a number of parallel suboperations (moduli) that are of smaller computational complexity. A much higher direction finding spatial resolution is achieved after the *N* different moduli are used and the results of the low precision suboperations are recombined, in addition to the reduction of the number of possible encoding errors due to the RSNS' inherent Gray-coding properties. This has resulted in a four inch antenna array being able to attain an angular resolution of less than 1.8 degrees with a continuous field of view of 120 degrees. The accompanying electronics occupy two 6 inch by 8 inch printed circuit boards, making this system ideal for platforms with limited space and volume.

KEYWORDS: Robust Symmetrical Number System, Phase Sampling Interferometry, Direction Finding, Ambiguity Resolution, Antennas

VHDL MODELING AND SIMULATION FOR A DIGITAL TARGET IMAGING ARCHITECTURE FOR MULTIPLE LARGE TARGETS GENERATION

Håkan P.I. Bergön-Major, Swedish Army
A.S., Swedish National Defence College, 2000
Master of Science in Systems Engineering-September 2002
Master of Science in Software Engineering-September 2002
Advisor: Douglas J. Fouts, Department of Electrical and Computer Engineering
Co-Advisor: Man-Tak Shing, Department of Computer Science
Co-Advisor: Phillip E. Pace, Department of Electrical and Computer Engineering

The subject of this thesis is to model and verify the correctness of the architecture of the Digital Image Synthesizer (DIS). The DIS, a system-on-a-chip, is especially useful as a counter-targeting repeater. It synthesizes the characteristic echo signature of a pre-selected target. The VHDL description of the DIS architecture was exported from Tanner S-Edit, modified, and simulated. Different software oriented verification approaches were researched and a White-box approach to functional verification was adopted. An algorithm based on the hardware functionality was developed to compare expected and simulated results. Initially, the architecture of one Range Bin Modulator was exported. Modifications to the VHDL source code included modeling of the behavior of the N-FET and P-FET transistors as well as Ground and Vdd (the voltages connected to the drains of the FETs). It also included renaming of entities to comply with VHDL naming conventions. Simulation results were compared to manual calculations and Matlab programs to verify the architecture. The procedure was repeated for the architecture of an Eight-Range Bin Modulator with equally successful results. VHDL was then used to create a super class of a 32-Range Bin Modulator. Test vectors developed in Matlab were used to yet again verify correct functionality.

KEYWORDS: Digital Image Synthesizer, Counter-Targeting Repeater, Range Bin Modulator, VHDL, White-box, Matlab

ADVANCED DENIAL OF SERVICE TECHNIQUES IN IEEE 802.11B WIRELESS LOCAL AREA NETWORKS

Robert W. Boshonek-Lieutenant, United States Navy
B.S., Strayer College, 1995
Master of Science in Systems Engineering-September 2002
Advisor: John McEachen, Department of Electrical and Computer Engineering
Second Reader: Dan Boger, Department of Information Science

The Institute of Electrical and Electronics Engineers (IEEE) Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications was designed and developed with three basic functionalities that are intended to minimize disruption or interference with coexisting systems. The IEEE has defined three physical (PHY) layer specifications, a medium access control (MAC) sublayer, and MAC management protocols and services. Specifically, the IEEE 802.11b standard uses a Digital Sequence Spread Spectrum (DSSS) transmission technique for the PHY layer and a MAC sublayer access control mechanism known as carrier sense multiple access/collision avoidance (CSMA/CA) with binary exponential backoff. The MAC management protocols and services element incorporates authentication/deauthentication and association/ disassociation functionality. This thesis demonstrates that all three of these protection mechanisms have inherent vulnerabilities that make the IEEE 802.11b standard susceptible to Denial of Service (DoS) exploitation.

KEYWORDS: Wireless Security, IEEE 802.11, IEEE 802.11b, Denial of Service, Distributed Coordination Function, Deauthentication, Disassociation, Request to Send

DESIGN OF AN ULTRA-WIDEBAND OMNI-DIRECTIONAL COMMUNICATIONS / JAMMER ANTENNA FOR THE NORTHROP-GRUMMAN EA-6B PROWLER AIRCRAFT

Vicente L. Cejoco-Commander, Philippine Navy
B.S. Philippine Military Academy, Baguio, 1982
B.S.E.C.E., Central Colleges of the Philippines, Manila 1995
Master of Science in Systems Engineering-September 2002
Advisor: Jovan E. Lebaric, Department of Electrical and Computer Engineering
Second Reader: Richard W. Adler, Department of Electrical and Computer Engineering

The Grumman EA-6B aircraft, which uses broadband communications and EW systems, needs an efficient, omni-directional and ultra-wideband antenna. Existing "blade" antennas have bandwidth limitations up to 500 MHz and unacceptable VSWR of 5.7:1 below 140 MHz, reducing the total effective bandwidth to 360 MHz. Previous studies suggested using dielectric cladding to reduce the physical size and aerodynamic loads and impedance matching circuits to improve VSWR. Previous antenna designs satisfy VSWR and radiation efficiency criteria but failed in the aerodynamic efficiency criteria due to large sizes making them impractical for installation onboard EA-6B whose speed approaches Mach 0.9. Rockwell-Collins, the manufacturer of the USQ-113 equipment installed aboard EA-6B has a new generation of jammers with extended frequency ranges up to 2.5 GHz. This development makes the blade antenna useless for higher frequency bands.

This thesis aims to design an ultra-wideband, vertically-polarized, omni-directional antenna which needs no dielectric cladding nor impedance matching circuits to satisfy the minimum acceptable VSWR criteria of 3:1, subject to strict dimension constraints while at the same time optimizing the aerodynamic performance. The electromagnetic portion of the antenna design and simulation was implemented using the CST Microwave Studio Finite Difference Time Domain (FDTD) Analysis software, while the antenna radome's aerodynamic parameters were derived using the Unsteady Potential Computational Fluid Dynamics (UPOT-CFD) software developed by the NPS Aeronautics and Astronautics Department. Applying basic principles of aircraft flight and the derived aerodynamic parameters, a short MATLAB code was written to facilitate the calculation of the aerodynamic drag, lift and bending moments acting on the radome structure. The optimal configuration is an "elliptic monocone" with two hollow ceramic resistive rods at both ends, purposely installed to add physical strength and to lower the VSWR. It can fully cover the entire 2.5GHz band, with a maximum VSWR of only 2.94:1 at 20 MHz, indicating an overall improvement of 2,140 MHz or almost six-fold the bandwidth coverage of the existing antenna.

KEYWORDS: Electronic Warfare, Ultra-wideband, Jammer Antenna, EA-6B Aircraft, Elliptic Monocone, Airborne Combat Antenna, FDTD Electromagnetic Modeling, Simulation, UPOT–CFD Aerodynamic Analysis Software, Radome

UTILIZATION OF THE EA-6B FOR AIRCRAFT CARRIER ANTI-SHIP MISSILE DEFENSE (ASMD) (U)

William W. Cox-Lieutenant Commander, United States Navy
B.S., Tulane University, 1989
Master of Science in Systems Engineering-September 2002
Advisor: D. Curtis Schleher, Department of Information Science
Second Reader: David C. Jenn, Department of Electrical and Computer Engineering

(U) The advent and proliferation of sophisticated anti-ship cruise missiles requires continued development of anti-ship missile defense tactics and theory. Relatively new and developing anti-ship cruise missile features such as home-on-radiation/jam, frequency agility, small radar cross-sections, challenging flight profiles, terminal anti-engagement maneuvering, delayed seeker turn-on, and more make detection, engagement and defense very difficult. The EA-6B Prowler aircraft is a viable addition to protection against these new types of anti-ship cruise missile. In particular, aircraft carriers may require alternative forms of protection, such as may be available by the EA-6B, due to its extremely large radar cross section. This thesis addresses the potential use of the EA-6B against threat missiles in defense of an aircraft carrier, evaluates the pros and cons of using the EA-6B in this role, and provides a preliminary tactics memorandum (TACMEMO) for future testing and development.

KEYWORDS: Antiship Cruise Missiles, Home-on-Jam, Jamming

ANALYSIS OF LOW PROBABILITY OF INTERCEPT (LPI) RADAR SIGNALS USING THE WIGNER DISTRIBUTION

Jen-Yu Gau-Captain, Taiwan Army
B.S., Chung-Cheng Institute of Technology, 1992
Master of Science in Systems Engineering-September 2002
Advisor: Phillip E. Pace, Department of Electrical and Computer Engineering
Second Reader: Herschel H. Loomis, Jr., Electrical and Computer Engineering

The parameters of Low Probability of Intercept (LPI) radar signals are hard to identify by using traditional periodogram signal processing techniques. Using the Wigner Distribution (WD), this thesis examines eight types of LPI radar signals. Signal to noise ratios of 0 dB and –6dB are also investigated.

The eight types LPI radar signals examined include Frequency Modulation Continuous Wave (FMCW), Frank code, P1 code, P2 code, P3 code, P4 code, COSTAS frequency hopping and Phase Shift Keying/Frequency Shift Keying (PSK/FSK) signals. This thesis also provides the Power Spectral Density (PSD), time domain, and Periodic Ambiguity Function (PAF) analysis to further characterize the LPI nature of the signals. Binary Phase Shift Keying (BPSK) signals although not LPI, are also examined to further illustrate the principal characteristics of the WD.

KEYWORDS: Low Probability of Intercept (LPI), Wigner Distribution (WD), Binary Phase Shift Keying (BPSK), Frequency Modulation Continuous Wave (FMCW), Polyphase, Frank, P1, P2, P3, P4, Costas Frequency Hopping, Phase Shift Keying/Frequency Shift Keying (PSK/FSK)

ANALYSIS OF LOW PROBABILITY OF INTERCEPT (LPI) RADAR SIGNALS USING CYCLOSTATIONARY PROCESSING

Antonio F. Lima, Jr.-Captain, Brazilian Air Force
B.S., Air Force Academy, 1993
Master of Science in Systems Engineering-September 2002
Advisor: Phillip E. Pace, Department of Electrical and Computer Engineering
Co-Advisor: Herschel H. Loomis, Jr., Department of Electrical and Computer Engineering

This thesis investigates the use of cyclostationary processing to extract the modulation parameters from a variety of continuous-wave (CW) low-probability-of-intercept (LPI) radar waveforms. The cyclostationary detection techniques described exploit the fact that digital signals vary in time with single or multiple periodicities, because they have spectral correlation, namely, non-zero correlation between certain frequency components, at certain frequency shifts. The use of cyclostationary signal processing in a non-cooperative intercept receiver can help identify the particular emitter and can help develop electronic attacks. LPI CW waveforms examined include Frank codes, polyphase codes (P1 through P4), Frequency Modulated CW (FMCW), Costas frequencies as well as several frequency-shift-keying/phase-shift-keying (FSK/PSK) waveforms. It is shown that for signal levels of 0dB and –6 dB, the cyclostationary signal processing can extract the modulation parameters necessary in order to distinguish between the various types of LPI modulations.

KEYWORDS: Low Probability of Intercept (LPI) Radars, Electronic Support (ES), Cyclostationary Processing, FFT Accumulation Method (FAM), Direct Frequency Smoothing Method (DFSM), Binary Phase Shift Keying (BPSK), Frequency Modulated Continuous Wave (FMCW), Polyphase Codes (P4, P3, P2, P1 and Frank Codes), Combined FSK/PSK (Frequency Shift Keying and Phase Shift Keying)

EXPLOITING IEEE 802.11B WIRELESS LOCAL AREA NETWORK SIGNALS FROM THE EP-3E

Benjamin Britten Massiglia-Lieutenant, United States Navy
B.S., Saint John's University, 1993
Master of Science in Systems Engineering-September 2002
Advisor: Tri T. Ha, Department of Electrical and Computer Engineering
Second Reader: Roy Radcliffe, Department of Electrical and Computer Engineering

Wireless technology continues to grow in functionality and popularity. This study explores the feasibility of using the EP-3E as a reconnaissance platform for exploiting IEEE 802.11b networks. It is an in-depth analysis of the propagation model for an IEEE 802.11b signal, the fundamental characteristics of an IEEE 802.11b packet data unit, the requirements for exploitation, and characteristics of an exploitation system. The study includes data collected from a prototype reconnaissance system including an aircraft, a notebook computer, software, cabling, and an amplifier.

KEYWORDS: Wireless Local Area Networks, IEEE 802.11b, EP-3E, MAC, PHY, Information Warfare

IEEE 802.11 WIRELESS LOCAL AREA NETWORK SECURITY THROUGH LOCATION AUTHENTICATION

J. D. Morrison-Lieutenant Commander, United States Navy
B.S., Virginia Tech, 1985
M.A., University of San Diego, 1995
Master of Science in Systems Engineering-September 2002
Thesis Advisor: J. D. Fulp, Department of Computer Science
Second Reader: Dan Boger, Department of Information Science

The IEEE 802.11b wireless Local Area Network architecture was designed to make associations between host access points and client mobile users as simple and fluid as possible. This gives the system tremendous flexibility, but results in vulnerability to illicit network connections by unauthorized users. The ability of network intruders with high gain antennas to establish anonymous connections while maintaining a comfortable stand off distance constitutes a threat that must be countered before operating a wireless LAN can be deemed an activity with acceptable risks.

This thesis explores the possibility of using relative position with respect to the network access point as the determining factor in granting network access to potential mobile users. By analyzing the latency of the layer two data acknowledgement control frames generated by the WLAN adapter card one should be able to infer the distance between the 802.11b access point and any particular mobile user. From this knowledge, a policy that excludes potential users beyond a specified range can be implemented.

KEYWORDS: Wireless Local Area Networks, WLAN, IEEE 802.11, 802.11b, Information Assurance, Network Security, War Driving

MODELING A NETWORKED TERRORIST ORGANIZATION WITH SITUATIONAL INFLUENCE ASSESSMENT MODULE (U)

Kenneth H. Morse-Captain, United States Air Force
B.A., University of Central Florida, 1993
Master of Science in Systems Engineering-September 2002
Robert V. Sanchez-Lieutenant, United States Navy
B.S., United States Naval Academy, 1995
Master of Science in Systems Engineering-September 2002
Advisor: Erik Jansen, Department of Information Science
Second Reader: LCDR Raymond Buettner, USN, Department of Information Science

(U)In recent years, the United States has been combating what seems to be a new type of terrorism. There have been numerous articles and books written about the "new terrorism" that discuss whether or not what

we are witnessing is indeed new. There is widespread agreement that terrorism is becoming more complex, transnational and networked. Because of this, terrorist organizations are increasingly difficult to analyze and target. This thesis uses computer modeling, specifically Situational Influence Assessment Module (SIAM), in an attempt to accurately predict those areas where the greatest influence can be exerted on a networked terrorist organization. Once known, combatant commanders can concentrate on these areas to influence the organization as national policy dictates. This thesis examines if a SIAM model has promise as a viable tool to analyze networked terrorist organizations. The joint staff and combatant commanders currently use SIAM to analyze complex strategic issues. The conclusion supported by this thesis is that SIAM is equally well suited for collaborative analysis of highly networked terrorist organizations.

KEYWORDS: Terrorism, Modeling, SIAM, Influence, Al Qaida

PROTOTYPING AND MEASUREMENTS OF AN ULTRA-WIDEBAND, TRANSMITTER-SAFE ANTENNA FOR THE USQ-146 INSTALLATION ON THE H-60 HELICOPTER

Neal M. Nottrott-Lieutenant Commander, United States Navy
B.A., Greenville College, Illinois, 1988
Master of Science in Systems Engineering-September 2002
Advisor: Jovan E. Lebaric, Department of Electrical and Computer Engineering
Second Reader: Richard W. Adler, Department of Electrical and Computer Engineering

The current configuration of the USQ-146 radio system on the H-60 helicopter uses two vertically polarized transmit antennas and one vertically-polarized receive antenna. The purpose of this design is to replace the two existing transmit antennas with vertically polarized ultra-wideband omni-directional antenna for use on an H-60 equipped with the USQ-146 radio system. The antenna should have a VSWR less than three, ideally less than two, over the frequency range of 20 – 2500 MHz. The antenna must mount through an existing cargo hole and maintain less than ten-inch ground clearance beneath the helicopter when landed. The antenna prototype is an enclosed, hollow, conical structure with three tube-style resistors evenly spaced around the base. This thesis develops a physical prototype for the antenna, measures the performance of the antenna with respect to VSWR, and compares these measurements with previously calculated computer simulations. The results for the prototype measurements show that the antenna operates within the desired frequency range, and that the VSWR remains safely within normal transmitter specifications.

KEYWORDS: Command, Control and Communications, Electronics, Sensors, Prototyping, Wideband Communications Antenna, Conical Antenna, Information Warfare, Transmitter-safe Antenna

NETWORK INTRUDER IDENTIFICATION VIA COVERT DATA EXFILTRATION USING LOCATION-AWARE CODE EMBEDDED IN A BENIGN SOFTWARE APPLICATION

Michael A. Schumann-Lieutenant Commander, United States Navy
B.A., Washington State University, 1991
Master of Science in Systems Engineering-September 2002
Advisor: J. Bret Michael, Department of Computer Science
Second Reader: LCDR Raymond Buettner, USN, Department of Information Science

This thesis details the development and demonstration of technical feasibility of a location-aware two-part software application. The term location-aware refers to knowing its location in relation to the IP address space.

A small section of code is hidden inside an apparently benign software application (henceforth referred to as the client). Another application (henceforth referred to as the server) runs as a daemon in Linux. The daemon updates, on a periodic basis, the client application's source code and executable with the current IP address of the host machine. This is accomplished through a dynamic algorithm that queries the current host machine's IP address and host name and actively patches and recompiles the client program's source code to reflect any changes.

If moved or copied to another system and subsequently executed, the client will gather identification information on the new host and covertly transmit the data back to the server application on the original host under the guise of performing benign file encryption and transfer. The collected information can be used to establish a network identification of the new host machine on which the client program has been executed.

KEYWORDS: Information Warfare, Network Security, Information Assurance

VULNERABILITY OF WLANS TO INTERCEPTION

Paul P. Sumagaysay-Lieutenant, United States Navy
B.A., University of San Diego, 1996
Master of Science in Systems Engineering-September 2002
Advisor: David C. Jenn, Department of Electrical and Computer Engineering
Second Reader: Phillip E. Pace, Department of Electrical and Computer Engineering

Wireless access is quickly broadening network reach by providing convenient and inexpensive access in hard-to-wire locations. As networks expand beyond defined boundaries, operators and managers are struggling to retain control over network usage and privacy. The signals from wireless communications systems and local area networks radiate in free space and therefore can be intercepted by terrorist operatives. Hidden receivers can be placed in public areas such as lobbies and parking lots outside of buildings. The signals are then intercepted or deception signals are injected into the wireless systems to jam or deceive. One solution is managing the RF transmission of the Wireless LAN. If the perpetrator can never intercept a signal from outside the boundary compounds of the network, then it is virtually impossible for the network to be hacked against. This thesis investigates the propagation of wireless signals in indoor and urban environments using computational electromagnetic codes available in the Department of Electrical and Computer Engineering's Microwave and Antenna Laboratory. The software was used to examine the vulnerability of these wireless systems and identify simple measures that can be taken to increase the system's security.

KEYWORDS: Wireless LAN Vulnerability, Antenna Propagation, Indoor-Outdoor Propagation

DETECTION AND CLASSIFICATION OF LOW PROBABILTY OF INTERCEPT RADAR SIGNALS USING PARALLEL FILTER ARRAYS AND HIGHER ORDER STATISTICS

Fernando L. Taboada-Major, Venezuelan Army
B.S., Armed Forces University, 1994
Master of Science in Systems Engineering-September 2002
Advisor: Phillip E. Pace, Department of Electrical and Computer Engineering
Co-Advisor: Herschel H. Loomis, Jr., Department of Electrical and Computer Engineering

This thesis first develops a MATLAB toolbox to generate important types of LPI waveforms based on frequency and phase modulation. The power spectral density and the periodic ambiguity function are examined for each waveform. These signals are then used to test a novel signal processing technique that detects the waveform parameters and classifies the intercepted signal in various degrees of noise. The technique is based on the use of parallel filter (sub-band) arrays and higher order statistics (third-order cumulant estimator). Each sub-band signal is treated individually and is followed by the third-order estimator in order to suppress any symmetrical noise that might be present. The significance of this technique is that it separates the LPI waveform in small frequency bands, providing a detailed time-frequency description of the unknown signal. Finally, the resulting output matrix is processed by a feature extraction routine to detect the waveform parameters. Identification of the signal is based on the modulation parameters detected.

KEYWORDS: Parallel Filter Arrays, Higher Order Statistics, Low Probability of Intercept Radar Signals, Frequency Modulated Continuous Wave, Polyphase Code

THE DESIGN AND ARCHITECTURE OF 2ND GENERATION HONEYNETS USING NETWORK DECEPTION

Jesus Torres, Jr.-Captain, United States Marine Corps
B.S., United States Naval Academy, 1996
Master of Science in Systems Engineering-September 2002
Advisor: John McEachen, Department of Electrical and Computer Engineering
Second Reader: Daniel F. Warren, Department of Computer Science

First generation Honeynets have served the purpose of allowing computer security professionals to analyze the tools and tactics used by hackers. Unfortunately, first generation Honeynets offer little protection to production systems and have primarily served as a research tool. Another drawback of first generation Honeynets is that they may require a lot of time in order to get compromised and usually do not reveal much information regarding the location of the attacker. Second generation Honeynets seek to provide a convincing "live" environment, with "real honey" for the attacker. Furthermore, second generation Honeynets seek to guide attackers into a specific area while providing some amount of protection to the production system(s). The use of a deception scheme, whether host-based or network based, produces significant challenges for the Honeynet administrators who must have a method for distinguishing between simulated events and events caused by the attacker. The experiments described in this thesis leverage the use of a tool called the Responder. Responder, a product of Fred Cohen & Associates, is the mechanism that seamlessly performs many forms of network deception in support of the 2nd Generation Honeynet.

KEYWORDS: Honeypot, Honeynet, Network Deception, 2nd Generation Honeynet, Responder, Fred Cohen

PERFORMANCE ANALYSIS OF A CDMA VSAT SYSTEM WITH CONVOLUTIONAL AND REED-SOLOMON CODING

Ugur Yigit-First Lieutenant, Turkish Army
B.S., Turkish Army Academy, 1997
Master of Science in Systems Engineering-September 2002
Advisor: Tri T. Ha, Department of Electrical and Computer Engineering
Second Reader: Herschel H. Loomis, Jr., Department of Electrical and Computer Engineering

The purpose of this thesis is to model a satellite communication system with VSATs, using Spread Spectrum CDMA methods and Forward Error Correction (FEC). Walsh codes and PN sequences are used to generate a CDMA system and FEC is used to further improve the performance. Convolutional and block coding methods are examined and the results are obtained for each different case, including concatenated use of the codes. The performance of the system is given in terms of Bit Error Rate (BER). As observed from the results, the performance is mainly affected by the number of users and the code rates.

KEYWORDS: VSAT, Digital Communications, Forward Error Correction, Convolutional Coding, Reed-Solomon Coding